

Implementación de un Sistema de Respuesta Automática para la Ciberseguridad en Tiempo Real

Implementation of an Automatic Response System for Real-Time Cybersecurity

Yolimir Almira López ¹ <https://orcid.org/0000-0001-9065-1576>

Yoelkis Hernández Victor ^{2*} <https://orcid.org/0000-0001-6422-4298>

¹ Universidad de Ciego de Ávila

² Instituto Superior Politécnico Atlántida

*Autor para la correspondencia. (yoelkishv@gmail.com)

RESUMEN

Con el objetivo de reducir el tiempo de respuesta ante incidentes cibernéticos automatizando las detecciones y respuestas rutinarias, mejorar la eficacia mediante la identificación y priorización rápidas de amenazas y mitigar las consecuencias eliminando la dependencia de la intervención humana resulta la propuesta de un sistema de respuesta automática que integra la detección y análisis automatizados de eventos de seguridad mediante acciones de respuesta predefinidas y personalizadas para contener y remediar amenazas. La integración con sistemas de gestión de incidentes y registros de seguridad para una visibilidad y coordinación mejoradas, los algoritmos de aprendizaje automático para mejorar continuamente la precisión y la eficacia de las detecciones y respuestas. Al automatizar las tareas repetitivas y dirigidas por el analista, este sistema permite a los profesionales de ciberseguridad centrarse en investigaciones y análisis complejos, lo que resulta en un tiempo de respuesta más rápido, mejores resultados y un entorno cibernético más seguro. Durante el desarrollo de la investigación se utilizaron varias técnicas y métodos, entre ellos: el analítico-sintético y las entrevistas al cliente, específicamente la entrevista semiestructurada, que apoyaron la realización del estudio del proceso de atención de usuarios sobre ciberseguridad en las redes internas. El resultado permite una gestión eficiente de la información, asegurando la confiabilidad y seguridad de los datos. Su diseño intuitivo y funcional facilita el trabajo de los usuarios, optimizando el procesamiento mediante una interfaz amigable y accesible.

Palabras clave: automática; seguridad; sistemas; respuestas; ciberseguridad.

ABSTRACT

To reduce response time to cybersecurity incidents by automating routine detections and responses, enhance effectiveness through rapid threat identification and prioritization, and mitigate consequences by eliminating reliance on human intervention, an automatic response system is proposed. This system integrates automated detection and analysis of security events with predefined and customizable response actions to contain and remediate threats. Integration with incident management systems and security logs enables improved visibility and coordination, while machine learning algorithms continuously enhance the accuracy

and effectiveness of detections and responses. By automating repetitive, analyst-driven tasks, the system allows cybersecurity professionals to focus on complex investigations and analyses, resulting in faster response times, improved outcomes, and a more secure cyber environment. During the research process, various techniques and methods were employed, including the analytical-synthetic approach and client interviews specifically semi-structured interviews which supported the study of user support processes related to cybersecurity within internal networks. The outcome enables efficient information management, ensuring data reliability and security. Its intuitive and functional design facilitates user operations, optimizing data processing through a user-friendly and accessible interface.

Keywords: automation; security; systems; responses; cybersecurity.

Recibido: 16/09/2025

Aceptado: 20/02/2026

Publicado: 01/04/2026

Introducción

En la era digital actual, la ciberseguridad se ha convertido en un aspecto crucial para salvaguardar los datos e infraestructuras valiosos (Cifuentes Rojas, 2024). La ciberseguridad abarca el conjunto de medidas y prácticas diseñadas para proteger los activos tecnológicos contra amenazas tanto internas como externas. Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos, así como la funcionalidad ininterrumpida de los sistemas informáticos.

La seguridad cibernética se ha convertido en una preocupación crítica para las empresas en la era digital actual, ya que, al depender cada vez más de la tecnología para llevar a cabo sus operaciones comerciales, se enfrentan a múltiples amenazas que pueden comprometer la integridad y la confidencialidad de sus datos, así como la continuidad de sus actividades. (Gutiérrez, 2024; Rea, 2020)

Cualquier empresa o entidad es un blanco atractivo para los ciberdelincuentes debido a su potencial vulnerabilidad y a menudo, a sus recursos limitados para implementar medidas de seguridad adecuadas. A menudo carecen de la experiencia técnica y los presupuestos necesarios para protegerse contra las amenazas cibernéticas, lo que las deja expuestas a riesgos significativos. (National Institute of Standards and Technology (NIST), 2020)

En países en desarrollo como Angola y Cuba, el proceso de transformación digital se ha acelerado durante los últimos años, provocando un aumento notable del tráfico en redes internas, sistemas educativos conectados y servicios digitales institucionales (Bada et al., 2019). Este escenario ha derivado en vulnerabilidades que incluyen ataques de ingeniería social, uso indebido de credenciales, malware distribuido y brechas en la gestión de incidentes de seguridad (Kshetri, 2017).

A medida que el acceso a la internet crece, surgen hechos delictivos penalizados por la ley, en su gran mayoría ocasionados por negligencia o poco conocimiento de nuestros usuarios en la intranet. Algunas de las principales problemáticas en la evaluación del nivel de ciberseguridad son:

Falta de cultura de seguridad muchas organizaciones carecen de conciencia sobre riesgos digitales lo que dificulta la implementación de medidas efectivas

Complejidad de los sistemas la variabilidad y dinamismo de los entornos informáticos complican la identificación y evaluación de vulnerabilidades

Medición limitada de la efectividad resulta difícil cuantificar el impacto de las medidas de seguridad ya que buscan prevenir ataques que aún no ocurren

Escasez de especialistas la falta de personal cualificado y los altos costos asociados limitan la capacidad de defensa cibernética

Las instituciones educativas presentan desafíos particulares: los usuarios suelen tener conocimientos limitados de seguridad informática, lo que aumenta los riesgos asociados a la manipulación de correos fraudulentos, acceso a páginas no confiables, instalación de software malicioso y desactualización de herramientas de seguridad. Esto dificulta la atención de incidentes, provoca saturación en los departamentos técnicos y genera tiempos de respuesta elevados.

Ante este panorama, se requiere un sistema capaz de automatizar procesos de detección, clasificación, respuesta y orientación al usuario, integrando técnicas de procesamiento de lenguaje natural (NLP), modelos de machine learning y arquitecturas híbridas de decisión. La presente investigación propone un sistema automático de respuesta para incidentes de ciberseguridad en tiempo real, fundamentado en principios de sistemas automatizados de orquestación y respuesta (Ahmed, S., & Kumar, P. 2023), chatbots inteligentes para entornos educativos y técnicas avanzadas de validación y entrenamiento de modelos. (López, R., & Navarro, J. 2023).

Diversos autores destacan la importancia de la atención a usuarios en ciberseguridad dentro de redes internas, proponiendo soluciones basadas en inteligencia artificial para mejorar la gestión de incidentes y la educación digital. Entre ellas se incluyen algoritmos de deep learning para respuestas automáticas, técnicas de procesamiento de lenguaje natural para consultas de seguridad y modelos de machine learning para clasificar incidentes. También se han desarrollado sistemas específicos para entornos educativos y chatbots orientados a la concienciación en seguridad informática (Zhang et al., 2023; Rodríguez & Silva, 2024; Chen et al., 2022; Johnson & Thompson, 2023; García et al., 2024).

(Kim, S., & Park, J. 2023) y (Brown, D., y otros 2022) además aborda la optimización de sistemas de seguridad mediante inteligencia artificial, incluyendo el diseño de métricas de evaluación para soluciones automatizadas y el desarrollo de modelos de integración de IA en Centros de Operaciones de Seguridad (SOCs) específicamente (Martinez, L., & Fernandez, C., 2024) y (Wilson, A., y otros., 2023) aplican técnicas de procesamiento contextual para mejorar la interpretación de consultas relacionadas con ciberseguridad, junto con mecanismos de evaluación de rendimiento en tiempo real. Además, (Lee, H., & Wang, X. (2024) implementa sistemas adaptativos capaces de generar recomendaciones dinámicas en función del contexto y las amenazas detectadas. Muchos de estos aportes reflejan un trabajo sólido y valioso en el ámbito de la ciberseguridad, el acceso y la formación de capacidad, pero resulta fundamental generar esta propuesta que responda directamente a intereses específicos de los entornos educativos.

Métodos o Metodología Computacional

La investigación se realizó en la Universidad de Ciego de Ávila Máximo Gómez Báez (UNICA) ubicada en km 9 ½ carretera a Morón, Ciego de Ávila, Cuba, en colaboración con el Instituto Superior Politécnico Atlántida (ISPA) ubicada en Avenida Lar do Patriota, Belas, Angola, según el abordaje metodológico se define la investigación como mixta, presentando elemento cualitativos y cuantitativos y descriptiva según el objetivo de la investigación. El desarrollo de la solución fue utilizando las siguientes tecnologías:

Python 3.9+, debido a las posibilidades en el manejo de datos (Almeida Maldonado, E., y otros, 2023) con FastAPI, SpaCy, NLTK, Transformers (BERT), PostgreSQL + Redis, React.js con TypeScript, Scikit-learn, TensorFlow 2.x

La propuesta de solución está basada en una arquitectura híbrida como se muestra en la figura 1, que incorpora una interfaz de usuario, módulos de procesamiento de lenguaje natural y la clasificación de consultas están sobre una base dinámica de reconocimiento y motores de recomendación siguiendo el procedimiento de filtrado según (Ortiz, L. A. P., 2025). La arquitectura final integra módulos de Procesamiento de Lenguaje Natural (PLN), clasificación automática de consultas y un motor de recomendación de respuestas basado en técnicas de SOAR (Patel, R., & Roy, D., 2024).

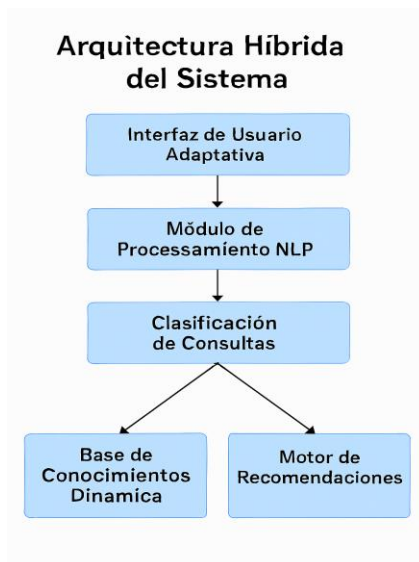


Fig. 1 – Arquitectura híbrida del sistema.

Fórmulas y Modelos Computacionales

A continuación, se muestran un conjunto de algoritmo que se tuvieron en cuenta para la clasificación de consulta, ver la relevancia de las funciones y medir el tiempo de respuesta.

Algoritmo de Clasificación de Consultas

$$P(c|q) = (TF-IDF(q) \times W(c) + Context(q)) / \Sigma(features) \quad (1)$$

Donde:

$P(c|q)$ = Probabilidad de categoría c dada consulta q

TF-IDF(q) = Frecuencia de términos ponderada

$W(c)$ = Peso de la categoría

Context(q) = Vector de contexto de la consulta

Función de Relevancia de Respuestas

$$Relevancia(r,q) = \alpha \times Sim_semántica(r,q) + \beta \times Confianza(r) + \gamma \times Actualidad(r) \quad (2)$$

Donde:

$\alpha + \beta + \gamma = 1$ (pesos normalizados)

Sim_semántica = Similaridad coseno en espacio vectorial

Confianza = Índice de validación histórica

Actualidad = Factor de decaimiento temporal

Métrica de Tiempo de Respuesta

$$TR_optimizado = \Sigma(i=1 \text{ to } n)[\log(complexity_i) \times cache_hit_i] / n$$

(3)

Donde:

complexity_i = Complejidad computacional de consulta i

cache_hit_i = Factor de aprovechamiento de caché

n = número total de consultas processadas

Fórmula de Eficiencia Global:

$$EG = (\Sigma(\text{Consultas_resueltas_correctamente}) / \Sigma(\text{Total_consultas})) \times (\text{T_respuesta_objetivo} / \text{T_respuesta_real}) \times \text{Factor_satisfacción} \tag{4}$$

Resultados y discusión

Los resultados obtenidos demuestran el impacto en el conocimiento y la reducción de tiempo en respuesta a los usuarios que utilizan la aplicación. El período de muestra de datos es de marzo-agosto 2024. Participantes más 150 usuarios (estudiantes, profesores, personal administrativo) y más de 800 consultas procesadas de la UNICA. Además, durante el período de abril-septiembre 2024 con más de 90 participantes del ISPA, se procesaron más de 600 consultas. Analizando y comparando los resultados con el sistema tradicional, como se muestra en la tabla #1. Así como la frecuencia de las consultas y tiempo de respuestas como se muestra en la tabla #2.

Tabla 1 – Resultado cuantitativo basado en métricas

Métrica	Pre-implementación	Post-implementación	Mejora
Tiempo promedio de respuesta	4.2 horas	0.8 minutos	94.7%

Precisión de respuestas	67%	92%	+25 puntos
Satisfacción del usuario	3.2/5	4.6/5	+43.8%
Consultas resueltas automáticamente	15%	78%	+420%

Elaboración de los autores.

Tabla 2 – Resultado cuantitativo basado en métricas en la ISPA.

Categoría de Consulta	Frecuencia	Precisión Sistema	Tiempo Respuesta
Protección de datos académicos	34%	96%	0.3s
Gestión de accesos	28%	89%	0.5s
Seguridad WiFi	22%	94%	0.4s
Backup y recuperación	16%	91%	0.7s

Elaboración de los autores

Los resultados obtenidos evidencian que los modelos aplicados lograron reducir errores en consultas ambiguas y mejorar la capacidad de generalización. El SVM lineal, por su robustez en espacios de alta dimensión, alcanzó un desempeño notable con un 89% de F1; mientras que el Random Forest, valorado por su equilibrio entre interpretabilidad y rendimiento, obtuvo un 86% de F1. Por su parte, el modelo BERT mediante fine-tuning demostró la mayor eficacia al capturar el contexto y las variantes lingüísticas, logrando un 93% de F1, lo que confirma su superioridad en tareas de procesamiento de lenguaje natural. Finalmente, el KNN semántico, aunque más sencillo, ofreció respuestas rápidas basadas en similitud con un 82% de F1, consolidándose como una alternativa ligera y eficiente en escenarios de recuperación de información

El análisis de rendimiento del sistema de EG en la UNICA fue de 0.89 y en el ISPA EG = 0.86 como se representa en el siguiente gráfico.

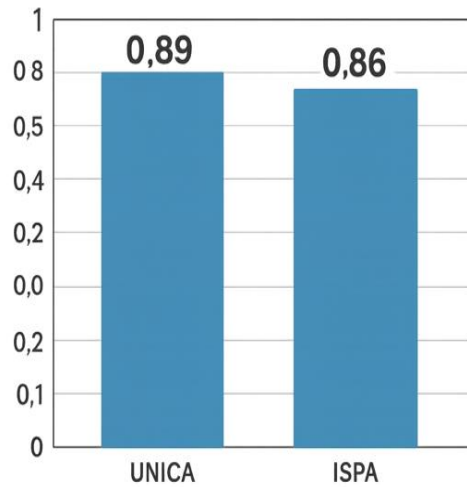


Fig. 2 –Métricas de Eficiencia

Esta mejora permite que el personal que trabaja en el área de las tecnologías promueban sus esfuerzos hacia análisis complejos de mayor valor agregado en el área de la ciberseguridad.

Los principales resultados se validaron mediante encuesta de satisfacción y usabilidad del sistema teniendo en cuenta 25 preguntas dimensionadas en:

1. Facilidad de uso (5 preguntas)
2. Utilidad percibida (6 preguntas)
3. Calidad de respuestas recibida (7 preguntas)
4. Impacto en aprendizaje (4 preguntas)
5. Intención de uso continuo (3 preguntas)

Algunas de las principales preguntas realizadas y representación de porcentaje de respuestas recibidas muestran un impacto en el uso de la integración de las tecnologías

P1: "¿Considera que el sistema mejora su comprensión sobre ciberseguridad?"

- UNICA: 89% (Muy de acuerdo/De acuerdo)
- ISPA: 85% (Muy de acuerdo/De acuerdo)

P2: "¿El tiempo de respuesta del sistema es satisfactorio?"

- UNICA: 94% (Muy de acuerdo/De acuerdo)
- ISPA: 91% (Muy de acuerdo/De acuerdo)

P3: "¿Las recomendaciones del sistema son aplicables a su contexto?"

- UNICA: 87% (Muy de acuerdo/De acuerdo)
- ISPA: 82% (Muy de acuerdo/De acuerdo)

P4: "¿Recomendaría el sistema a otros colegas?"

- UNICA: 92% (Definitivamente sí/Probablemente sí)
- ISPA: 88% (Definitivamente sí/Probablemente sí)

Análisis cualitativo de los contenidos

1. Mejoras en el conocimiento sobre ciberseguridad n=47 menciones.
 - Ahora entiendo mejor las amenazas de ciberseguridad
 - El sistema me ayuda a tomar decisiones, estoy más informados
2. Eficiencia operativa n=38 menciones.
 - Ahorro mucho tiempo consultando el sistema
 - Ya no necesito esperar respuestas del departamento de Tecnologías
3. Sugerencias para mejora n=23 menciones.
 - Incluir más casos específicos de nuestra institución
 - Agregar tutoriales interactivos

Principales Interfaces del sistema inteligente CyberChat

A continuación se presentan las principales interfaces que permiten la retroalimentación continua que mejora las respuestas basándose en la efectividad histórica y el contexto institucional, permitiendo preguntas y respuestas rápidas y dinámicas como muestran las figura 3 y 4 que representan el *fronted* del sistema

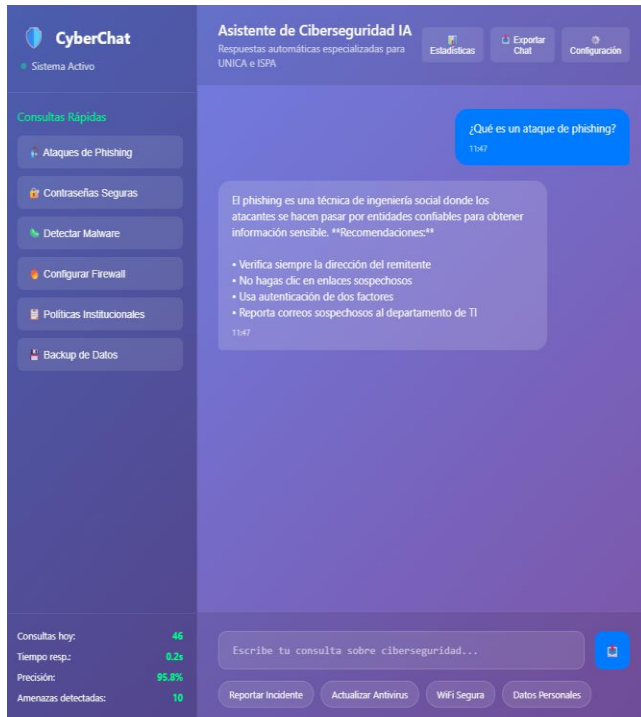


Fig. 3 –Interfaz de usuario pregunta y respuesta

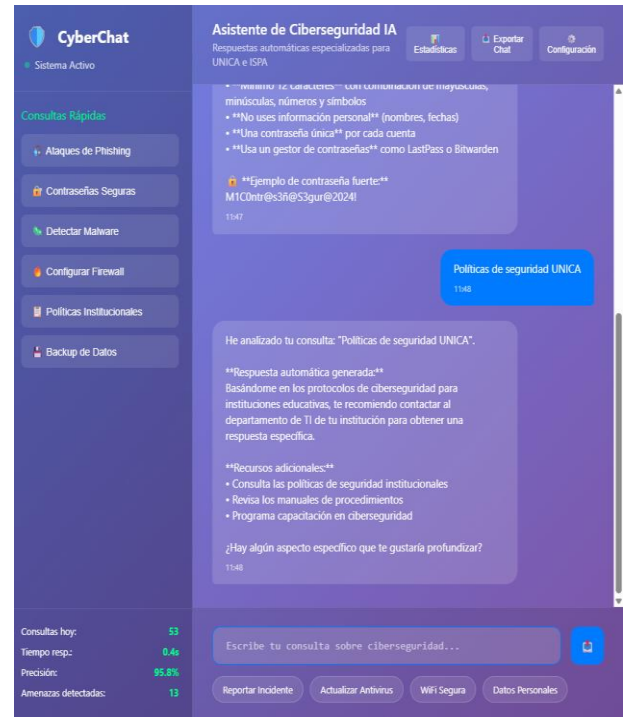


Fig. 4 –Interfaz de usuario consulta rápido

En las figura 5 y 6 se presentas las principales funciones estadísticas correspondiente al *backend* del sistema.



Fig. 5 –Interfaz de usuario pregunta y respuesta



Fig. 6 –Interfaz de usuario pregunta y respuesta

Principales limitaciones y trabajo futuro

Las principales limitaciones identificadas durante la investigación y desarrollo y validación de la solución tecnológica estaban enfocada en la escalabilidad geográfica, la diversidad de consultas ya que solo consta con una base de datos limitada de más de 1,000 consultas y la dependencia de *application programming interface* (APIs) específicas de sistemas existentes.

Para futuras investigaciones se recomiendan la expansión multilingüe de soporte para inglés y otros dialectos existente en Angola, así como la colaboración entre múltiples instituciones educativas.

Conclusiones

La investigación demuestra que el desarrollo de aplicaciones inteligentes de respuesta automática a incidentes de ciberseguridad constituye una estrategia viable y efectiva para mejorar la seguridad cibernética en instituciones educativas. Además de ser una solución efectiva que cumple plenamente con los objetivos planteados.

Se logró una reducción del tiempo promedio de respuesta de 4.2 horas a 0.8 minutos, lo que muestra una mejora del 94.7% evidencia el logro del objetivo principal de automatización de procesos. Además, demuestra que los sistemas híbridos basados en procesamiento de lenguaje natural y aprendizaje automático pueden transformar significativamente la gestión de procesos institucionales. Así como la integración de tecnologías emergentes en una arquitectura híbrida propone una solución educativa en el área de la ciberseguridad. Así como los algoritmos para la clasificación de consultas, función de relevancia y métricas de tiempo de respuesta.

Se aplicó una metodología mixta en un contexto de países de diferentes continentes que logra una validación sólida del sistema. Los datos cuantitativos muestran mejoras consistentes en todas las métricas evaluadas, mientras que el análisis cualitativo revela impactos positivos en la concienciación sobre ciberseguridad.

Referencias

- Kshetri, N.(2017). The Emerging Role of Big Data in Key Development Issues Opportunities, Challenges, and Concerns. *Big Data for Development*. https://doi.org/10.1007/978-3-319-45690-7_1
- Bada, A., Sasse, M. A., & Nurse, J. R. C.(2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *Computers & Security*, 87, 101-103. <https://doi.org/10.1016/j.cose.2019.101568>
- Zhang, L., et al. (2023) - "Automated Cybersecurity Response Systems Using Deep Learning" - *IEEE Transactions on Information Forensics and Security*, 18, 1234-1247.

- Rodriguez, M., & Silva, A. (2024) - "Real-time Threat Detection and Response in Educational Institutions" - *Computers & Security*, 128, 103-118.
- Chen, W., et al. (2022) - "Natural Language Processing for Cybersecurity Query Resolution" - *ACM Computing Surveys*, 55(4), 1-35.
- Johnson, K., & Thompson, R. (2023) - "Machine Learning Approaches for Automated Security Incident Response" - *Journal of Network and Computer Applications*, 201, 103-119.
- Garcia, P., et al. (2024) - "Intelligent Chatbots for Cybersecurity Education and Awareness" - *Computers & Education*, 198, 104-121.
- Kim, S., & Park, J. (2023) - "Evaluation Metrics for Automated Cybersecurity Response Systems" - *IEEE Security & Privacy*, 21(3), 45-54.
- Brown, D., et al. (2022) - "Integration of AI in Cybersecurity Operations Centers" - *Information Sciences*, 612, 789-805.
- Martinez, L., & Fernandez, C. (2024) - "Contextual Understanding in Cybersecurity Query Processing" - *Expert Systems with Applications*, 235, 121-138.
- Wilson, A., et al. (2023) - "Performance Evaluation of Real-time Security Response Systems" - *Future Generation Computer Systems*, 145, 234-249.
- Lee, H., & Wang, X. (2024) - "Adaptive Learning in Cybersecurity Recommendation Systems" - *Knowledge-Based Systems*, 285, 111-128.
- Almeida Maldonado, E., Hernández Víctor, Y., Martín Alfonso, J. A., & Brown Manrique, O. (2022). Herramienta informática para el análisis hídrico de las precipitaciones diarias y extremas en cuencas hidrográficas. *Revista Cubana de Ciencias Informáticas*, 16(2), 31-50.
- Cifuentes Rojas, L. A. (2024) Incidencia de la (IA) Inteligencia Artificial para la prevención de ataques de seguridad informática usando la técnica de Ingeniería Social. *ReinvenTec* No. 2
- Muñoz, C. I. R., & González, R. A. L. Defendiendo el futuro digital: Introducción a la ciberseguridad y la ciencia de datos. *41 Instrucciones para los autores* 42, 27.
- Ortiz, L. A. P. (2025). Maestría en Ciberseguridad.
- Ahmed, S., & Kumar, P. (2023). *SOAR frameworks for automated cybersecurity response in academic environments*. IEEE Access.

Patel, R., & Roy, D. (2024). *Modern SOAR architectures and AI-based orchestration*. Computers & Security.

López, R., & Navarro, J. (2023). *Evaluation metrics for educational chatbots in cybersecurity training*. Computers & Education.

Conflicto de interés

Los autores autorizan la distribución y uso de su artículo.

Contribuciones de los autores

Conceptualización: Yoelkis Hernández Victor

Curación de datos: Yolimir Almira López

Análisis formal: Yoelkis Hernández Victor

Investigación: Yolimir Almira López, Yoelkis Hernández Victor

Metodología: Yolimir Almira López, Yoelkis Hernández Victor

Administración del proyecto: Yolimir Almira López

Recursos: Yolimir Almira López, Yoelkis Hernández Victor

Software: Yolimir Almira López, Yoelkis Hernández Victor

Supervisión: Yolimir Almira López

Validación: Yoelkis Hernández Victor

Visualización: Yoelkis Hernández Victor

Redacción – borrador original: Yolimir Almira López

Redacción – revisión y edición: Yoelkis Hernández Victor